



9110-9B

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2016-0002]

Privacy Act of 1974; Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to update and reissue a current Department-wide system of records titled, “Department of Homeland Security(DHS)/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records,” 76 FR 39408, July 6, 2011. This system of records allows the DHS to maintain a synchronized copy of the Department of Justice’s (DOJ) Federal Bureau of Investigation’s (FBI) Terrorist Screening Database (TSDB), which includes categories of individuals covered by DOJ/FBI-019, “Terrorist Screening Records Center System,” 72 FR 77846, Dec. 14, 2011. DHS maintains a synchronized copy to automate and simplify the transmission of information in the Terrorist Screening Database to DHS and its components. With this updated notice, DHS is adding two new consumers, Customs and Border Protection (CBP) Automated Targeting System (ATS) and U.S. Citizenship and Immigration Services (USCIS) Fraud Detection and National Security (FDNS) Directorate, to the “DHS Watchlist Service.” The DHS Watchlist Service is the technological mechanism used to transmit Terrorist Screening Database information from the Department of Justice to the Department of

Homeland Security, and to DHS components thereafter. DHS is also clarifying an existing category of individuals, adding two new categories of individuals, and clarifying the categories of records maintained in this system. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

DHS is also issuing a new notice of proposed rulemaking to cover the exemptions applied to these new categories of individuals covered by this system of records notice. The notice of proposed rulemaking will be published concurrently with this notice. The existing Final Rule for Privacy Act exemptions will continue to apply until the new Final Rule is published. This updated system will be included in DHS's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This updated system will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2016-0002 by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

DOCKET: For access to the docket to read background documents or comments received, please visit <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions and privacy issues please contact: Karen L. Neuman (202-343-1717), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) proposes to update and reissue the current system of records titled, “Department of Homeland Security (DHS)/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records.” DHS maintains a synchronized copy of the Department of Justice’s (DOJ) Federal Bureau of Investigation’s (FBI) Terrorist Screening Database (TSDB), which includes individuals covered by DOJ/FBI-019, “Terrorist Screening Records Center System,” 72 FR 77846, Dec. 14, 2011, via a technological mechanism called the “DHS Watchlist Service (WLS).” The DHS WLS disseminates received TSDB records to authorized DHS components.

Homeland Security Presidential Directive 6 (HSPD-6), issued in September 2003, called for the establishment and use of a single, consolidated watchlist to improve the identification and screening of known or suspected terrorists and their supporters. The FBI’s Terrorist Screening Center (TSC) maintains and distributes TSDB as the U.S.

Government's consolidated terrorist watchlist system. DHS and the FBI/TSC developed the WLS in order to automate and simplify the method for transmitting TSDB records from the FBI/TSC to DHS and its authorized components.

The WLS supports an automated and centralized data transmission of TSDB data to DHS and its components. The WLS replaced multiple data feeds from the FBI/TSC to DHS and its components, which were documented by information sharing agreements. The WLS is a system-to-system secure connection with no direct user interface.

DHS and its components are authorized to access TSDB records via the WLS pursuant to the terms of information sharing agreements with FBI/TSC. DHS is updating this SORN and has published privacy impact assessments to provide additional transparency into how DHS has implemented WLS. DHS will review and update this SORN no less than every two years as new DHS systems are interconnected with the WLS and are approved, consistent with the terms of agreements with FBI/TSC. There are currently six DHS systems authorized to receive TSDB data directly from the FBI/TSC via WLS, including two systems new to this SORN. The following systems have existing SORNs that permit the use of the TSDB:

- (1) Transportation Security Administration (TSA): "DHS/TSA-002 Transportation Security Threat Assessment System (T-STAS)," 79 FR 46862, Aug. 11, 2014;
- (2) TSA Secure Flight Program: "DHS/TSA-019 Secure Flight Records," 80 FR 233 Jan. 5, 2015;
- (3) U.S. Customs and Border Protection (CBP) Passenger Systems Program, as included in TECS: "DHS/CBP-011 TECS", 73 FR 77778, Dec. 19, 2008;

- (4) Office of Biometric Identity Management (OBIM), as included in the DHS Automated Biometric Identification System (IDENT): DHS/US-VISIT-004, “DHS Automated Biometric Identification System (IDENT),” 72 FR 31080, June 5, 2007.

DHS is expanding the use of the WLS within the Department to include two new systems with existing SORNs that cover the use of the TSDB:

- (5) CBP, DHS/CBP-006, “Customs and Border Protection Automated Targeting System,” 77 FR 30297, May 22, 2012;
- (6) U.S. Citizenship and Immigration Services (USCIS) Fraud Detection and National Security (FDNS) Directorate, as included in the FDNS-Data System, “DHS/USCIS-006 Fraud Detection and National Security Records” 77 FR 47411, Aug. 8, 2012.

Two other DHS components are authorized to receive TSDB data via the WLS in the form of a computer readable extract. The components’ use of the TSDB data is covered by existing SORNs:

- (1) DHS/IA-001, “Office of Intelligence and Analysis (I&A) Enterprise Records System,” 73 FR 28128, May 15, 2008; and
- (2) DHS/ICE-009, U.S. Immigration and Customs Enforcement’s (ICE) “ICE External Investigations,” 75 FR 404, Jan. 5, 2010.

Transactional Information stored in the WLS may be shared with the FBI/TSC in order to ensure that DHS and the FBI/TSC can reconcile any differences in the database and ensure DHS has the most up-to-date and accurate version of TSDB records, such as

through automated response messages from WLS to TSC. All other sharing will be conducted pursuant to the programmatic system of records notices.

DHS is also updating this system of records to clarify one category of individuals and add two new categories of individuals whose information is currently included in, or is contemplated for inclusion in, the TSDB. These categories of information have been included in the TSDB to in support of the White House's "Strategy to Combat Transnational Organized Crime" (July 19, 2011), and National Security Presidential Directive-59/Homeland Security Presidential Directive-24, "Biometrics for Identification and Screening to Enhance National Security" (June 5, 2008). These executive strategies are relevant to DHS's vetting and screening operations.

DHS is clarifying the category of individuals to explicitly include relatives, associates, or others closely connected with a known or suspected terrorist who are excludable from the United States based on these relationships by virtue of Section 212(a)(3)(B) of the Immigration and Nationality Act, as amended, and do not otherwise satisfy the requirements for inclusion in the TSDB.

DHS is adding two new categories of individuals to include: (1) individuals who were officially detained during military operations, but not as enemy prisoners of war, and who have been identified as possibly posing a threat to national security, and who do not otherwise satisfy the requirements for inclusion in the TSDB ("military detainees"), consistent with E.O. 12333 (or successor order) and the DOJ/FBI-019; and (2) individuals who may pose a threat to national security because they are (a) known or suspected to be or have been engaged in conduct constituting, in aid of, or related to transnational organized crime, thereby posing a possible threat to national security, and

(b) do not otherwise satisfy the requirements for inclusion in the TSDB (“transnational organized crime actors”), consistent with E. O. 12333 (or successor order) (“national security threats”) and in support of the White House’s “Strategy to Combat Transnational Organized Crime” (July 19, 2011), and National Security Presidential Directive-59/Homeland Security Presidential Directive-24, “Biometrics for Identification and Screening to Enhance National Security” (June 5, 2008).

DHS is updating this system of records to clarify and expand the categories of records maintained by the Department. These categories of records are types of data elements included in the TSDB and are shared with DHS and have been deemed relevant to supporting DHS’s vetting and screening operations.

1. Identifying biographic information, such as name, date of birth, place of birth, passport or driver’s license information, and any other available identifying particulars used to compare the identity of an individual being screened with a subject in the TSDB;
2. Biometric information, such as photographs, fingerprints, or iris images, and associated biographic and contextual information;
3. References to, or information from, other government law enforcement and intelligence databases, or other relevant databases that may contain terrorism and/or national security information, such as unique identification numbers used in other systems;
4. Information collected and compiled to maintain an audit trail of the activity of authorized users of WLS information systems; and

5. System-generated information, including metadata, archived records and record histories from WLS.

DHS is planning future enhancements to the WLS that will provide for a central mechanism to receive information from DHS components when they encounter a potential match to the TSDB and send this information to the FBI/TSC. DHS will update this SORN to reflect such enhancements to the WLS once that capability is implemented. All encounter-related information sharing from DHS to the FBI/TSC will be conducted pursuant to the programmatic system of records notices outlined above.

DHS previously published a Final Rule in the Federal Register to exempt this system of records from certain provisions of the Privacy Act at 75 FR 55335, Dec. 29, 2011. DHS is publishing a new notice of proposed rulemaking to cover the exemptions that will now be applied to these new categories of individuals covered within this system of records. The existing Final Rule for Privacy Act exemptions continues to apply until the new Final Rule is published. This updated system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to

encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records.

In accordance with 5 U.S.C. § 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

Department of Homeland Security (DHS)/ALL-030

System name:

DHS/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records

Security classification:

Unclassified.

System location:

Records are maintained at DHS and Component Headquarters in Washington, D.C. and field offices.

Categories of individuals covered by the system:

Categories of individuals covered by this system include:

- a) Individuals known or suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (“known or suspected terrorists”);

- b) Individuals who are foreign nationals or lawful permanent resident aliens and who are excludable from the United States based on their familial relationship, association, or connection with a known or suspected terrorist as described in Section 212(a)(3)(B) of the Immigration and Nationality Act of 1952 (“INA exceptions”);
- c) Individuals who were officially detained during military operations, but not as Enemy Prisoners of War, and who have been identified to pose an actual or possible threat to national security (“military detainees”); and
- d) Individuals known or suspected to be or have been engaged in conduct constituting, in aid of, or related to transnational organized crime, thereby posing a possible threat to national security (“transnational organized crime actors.”)

Categories of records in the system:

Categories of records in this system include:

1. Identifying biographic information, such as name, date of birth, place of birth, passport and/or driver’s license information, and other available identifying particulars used to compare the identity of an individual being screened with a subject in the TSDB;
2. Biometric information, such as photographs, fingerprints, or iris images, and associated biographic and contextual information;
3. References to or information from other government law enforcement and intelligence databases, or other relevant databases that may contain

terrorism or national security information, such as unique identification numbers used in other systems;

4. Information collected and compiled to maintain an audit trail of the activity of authorized users of WLS information systems; and
5. System-generated information, including metadata, archived records and record histories from WLS.

Authority for maintenance of the system:

Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135; The Tariff Act of 1930, Pub. L. 71-361, 46 Stat. 741, as amended; The Immigration and Nationality Act; 49 U.S.C. 114, 5103a, 40113, ch. 49 and 46105; Homeland Security Presidential Directive/HSPD-6, “Integration and Use of Screening Information to Protect Against Terrorism” (Sept. 16, 2003); Homeland Security Presidential Directive/HSPD-11, “Comprehensive Terrorist-Related Screening Procedures” (Aug. 27, 2004); National Security Presidential Directive/NSPD-59/Homeland Security Presidential Directive/HSPD-24, “Biometrics for Identification and Screening to Enhance National Security” (June 5, 2008); E.O. 13388, “Further Strengthening the Sharing of Terrorism Information to Protect Americans,” 70 FR 62023 (Oct. 25, 2005); Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108–458, 118 Stat 3638; National Security Act of 1947, Pub. L. 235, 61 Stat. 495, as amended; and 28 U.S.C. 533.

Purpose(s):

DHS and its components collect, use, maintain, and disseminate information in the DHS Watchlist Service (WLS) to facilitate DHS mission-related functions, such as counterterrorism, law enforcement, border security, and inspection activities. TSDB data,

which includes personally identifiable information (PII), is necessary for DHS to effectively and efficiently assess the risk or threat posed by a person for the conduct of its mission.

The Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC) provides a near real time, synchronized version of the TSDB to DHS in order to improve the timeliness and governance of watchlist data exchanged between the FBI's TSC and DHS and its component systems that currently use TSDB data.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ)/FBI/TSC in order to receive confirmations that the information has been appropriately transferred and any other information related to the reconciliation process so that DHS is able to maintain a synchronized copy of the TSDB.

DHS will share information contained in this system to components internal to DHS pursuant to subsection 552a(b)(1) of the Privacy Act, and subsequently may be shared externally outside DHS at the programmatic level pursuant to routine uses described in the following published system of records notices:

(1) DHS/TSA-002 Transportation Security Threat Assessment System (T-STAS), 79

FR 46862, Aug. 11, 2014;

(2) DHS/TSA-019 Secure Flight Records, 80 FR 223, Jan. 5, 2015;

- (3) DHS/CBP-011 TECS, 73 FR 77778, Dec. 19, 2008;
- (4) DHS/CBP-006, Customs and Border Protection Automated Targeting System, 77 FR 30297, May 22, 2012;
- (5) DHS/US-VISIT-004, DHS Automated Biometric Identification System (IDENT), 72 FR 31080, June 5, 2007;
- (6) DHS/IA-001, Office of Intelligence and Analysis (I&A) Enterprise Records System, 73 FR 28128, May 15, 2008;
- (7) DHS/ICE-009, ICE External Investigations, 75 FR 404, Jan. 5, 2010; and
- (8) DHS/USCIS-006 Fraud Detection and National Security Records, 77 FR 47411, Aug. 8, 2012.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

DHS stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on servers, magnetic disc, tape, digital media, and CD-ROM.

Retrievability:

DHS may retrieve records by name or other personal identifier.

Safeguards:

DHS safeguards records in this system in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies.

Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

The WLS maintains a near real time feed of the TSDB, and does not retain historical copies of the TSDB. The WLS is synchronized with the TSDB. When the FBI/TSC adds, modifies, or deletes data from the TSDB, the WLS duplicates these functions almost simultaneously, and that information is then passed to DHS and its authorized component systems. DHS does not manipulate the data within the TSDB feed received by WLS. The authorized DHS component that is screening individuals will maintain, separate from the WLS, a record of a match or possible match with the TSDB and DHS will retain this information in accordance with the DHS component specific SORNs identified in this notice.

System Manager and address:

Executive Director, Passenger Systems Program Directorate, Office of Information and Technology, U.S. Customs and Border Protection, 7400 Fullerton Rd, Springfield, VA 22153.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS and its components will consider individual requests to determine whether or not information may be released. Thus, individuals seeking

notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or component FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under “contacts.” If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 C.F.R. part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, <http://www.dhs.gov/foia> or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

In addition, if individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Inquiry Redress Program (DHS TRIP), 72 FR 2294, Jan. 18, 2007. Individuals who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by DHS may submit a redress request through DHS TRIP. The DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs such as airports and train stations or crossing U.S. borders. Redress requests should be sent to: DHS Traveler Redress Inquiry Program, 601 South 12th Street, TSA-901, Arlington, VA 20598 or online at <http://www.dhs.gov/trip> and at <http://www.dhs.gov>.

Record access procedures:

See “Notification procedure” above.

Contesting record procedures:

See “Notification procedure” above.

Record source categories:

Records are received from the FBI's Terrorist Screening Center, specifically records covered by DOJ/FBI-019 Terrorist Screening Records System, 72 FR 47073, Aug. 22, 2007.

Exemptions claimed for the system:

The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(1) and (k)(2).

Dated: January 12, 2016.

Karen L. Neuman
Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2016-01167 Filed: 1/21/2016 8:45 am; Publication Date: 1/22/2016]